UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,720	10/15/2003	Alan O'Neill	060576U2	5387

23696 7590 05/27/2008
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
OKORONKWO, CHINWENDU C	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
05/27/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	**Application No.** 10/685,720	**Applicant(s)** O'NEILL, ALAN	
	Examiner CHINWENDU C. OKORONKWO	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 February 2008_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-51_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-51_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _04/23/2008_.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 10/15/2007, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

1.1 Examiner acknowledges the cancellation of claims 15, 18 and 21 and subsequent overcoming of the 35 U.S.C 101 rejection of the previous Office Action.

Response to Remarks/Arguments

2. Applicant's arguments, pages 17-23, with respect to the rejection of claims 1-51 have been fully considered but they are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava (US 6,684,331 B1).

Regarding claims 1, 19, 22, 34, 43 and 47, Srivastava discloses a communications method for use in a system including comprising a first, second and third nodes, and a first secret, said first secret being shared between the first and second nodes to secure communications between said first and second nodes, the method comprising: operating the first node to establish a secure communications session with said second node using the first shared secret to secure the contents of packets communicated from the first node that are directed to the second node as part of the secure communications session; operating a third node which is coupled to said first and second nodes to maintain in memory a copy of said first shared secret; and operating the third node to receive a secure flow of packets from the first node that are directed to said second node as part of the secure communications session (figure 1, column 2 lines 27 – 41 and column 9 lines 38 – 49).

Srivastava is silent in disclosing packets communicated from the first node that are directed to the second node being addressed to said second node by use of a second node destination address, however it would have been obvious for one of ordinary skill in the art, at the time of the invention to have been motivated to modify the invention of Srivastava to teach packet communication from the disclosure of first node being directed to the second node. The basis/motivation for such modification is found in column 2 line 42-54 which recites – “scenario involves participants A and B, in which user A is considered a publisher of a message to a subscriber, user B,” the disclosure of participants A and B communicating messages between each other is understood as providing motivation for claiming the “user A is considered a publisher of a message to a subscriber, user B,” the benefit of such modification being increased processing speed and packet transmission/communication.

Regarding claims 2, 20, 35,45 and 50, Srivastava discloses the method of claim 1, further comprising: operating the third node to receive from said second node the first shared secret and to store the first shared secret in memory, said received first shared secret being encrypted using a second shared secret known to the second and third nodes (column 12 lines 24 – 55).

Regarding claims 3, 21, 36, 46 and 51, Srivastava discloses the method of claim 2, further comprising: operating said third node to receive and process packets sent from said first node as part of said established communications session, said third node sending a message to the first node indicating successful receipt of packets by said second node (figure 4C and column 13 lines 63 – 67 and column 14 lines 1 – 17, column 10 lines 7 – 19).

Regarding claims 4, 24, 37, Srivastava discloses the method of claim 3, wherein said third node uses said first shared secret to secure the message to the first node (column 4 lines 4 – 17, column 9 lines 38 – 49).

Regarding claims 5, and 38, Srivastava discloses the method of claim 5, wherein said third node operates as an application proxy for said second node during said secure communications session without informing said first node that the third node is acting as a proxy in the place of said second node (Figure 2C column 7 lines 49 – 61 and column 8 lines 3 – 16 and column 10 lines 20 – 33).

Regarding claims 6, 26, 39 and 41, Srivastava discloses the method of claim 5, further comprising: operating the third node to transmit information obtained from said communications session while said third node was acting as a proxy for said second node to said second node; and operating the second node to continue the secure communications session with the first node (column 7 lines 49 – 61 and column 8 lines 3 – 16, column 10 lines 20 – 33, column 12 lines 24 – 55).

Regarding claims 7, 27, Srivastava discloses the method of claim 1, further comprising: operating the third node to inspect the secure packet flow from the first node, said step of inspecting said secure packet flow including performing at least one of a group of security steps which use the first shared secret, said group of security steps comprising: decrypting a packet, integrity checking contents of a packet, and authenticating a sender of a packet (Figure 3 and column 11 lines 34 – 60).

Regarding claims 8, 28, Srivastava discloses the method of claim 7, further comprising: operating the third node to drop the packet from the packet flow if the performed at least one of the group of security checks fails (column 4 lines 4 – 17, column 9 lines 38 – 49).

Regarding claims 9, 29, Srivastava discloses the method of claim 7, further comprising: operating the third node to additionally process the packets from the packet flow if no performed security check in said group of security checks fails (column 7 lines 49 – 61 Figure 2C and column 10 lines 20 – 33, and column 8 lines 3 – 16).

Regarding claims 10, 30, Srivastava discloses the method of claim 9, further comprising: operating the third node to identify a packet with a disallowed packet payload by comparing at least a portion of the payload of each packet in the packet flow to information indicating allowed packet payloads, payloads of a type which are not indicated by said information being disallowed packet payloads (column 8 lines 17 – 60, column 11 lines 34 – 60).

Regarding claims 11, 31, Srivastava discloses the method of claim 10, further comprising: operating the third node to drop an identified packet with a disallowed packet payload fails (Figure 3 and column 11 lines 34 – 60, column 4 lines 4 – 17).

Regarding claims 12, 32, Srivastava discloses the method of claim 10, further comprising: operating the third node to modify the packet payload of packets identified to include a disallowed packet payload based on stored information indicating payload modifications to be made to disallowed packet payloads (column 4 lines 4 – 17, column 8 lines 17 – 60).

Regarding claims 13 and 33, Srivastava discloses the method of claim 12, wherein the modified payload generated by modifying a packet payload includes a message indicating that an erroneous payload was detected at the third node (figure 4C and column 13 lines 63 – 67, column 7 lines 49 – 61 and column 8 lines 3 – 16 and column 14 lines 1 – 17).

Regarding claim 14, Srivastava discloses the method of claim 10, further comprising: operating the third node to process at least two packets in the packet flow to produce at least a third packet (column 4 lines 4 – 17).

Regarding claim 15, Srivastava discloses the method of claim 9, further comprising; operating the third node to generate an additional packet flow from the received packet flow directed to the second node and to forward the additional packet flow to the second node, packets in said additional packet flow having a source address corresponding to the first node and a destination address corresponding to the second node, said step of generating an additional packet flow including at least one of a group of security steps which use the first shared secret, the group of security steps consisting of: encrypting a packet, adding an integrity check for the contents of the packet, and adding an authenticator check for the packet sender (column 7 lines 49 – 61 and column 8 lines 3 – 16).

Regarding claim 16, Srivastava discloses the method of claim 1, wherein the second and third nodes each include a second secret used to secure communications between the third node and the second node, the method further comprising: operating the third node to generate an additional packet flow from the received packet flow directed to the second node and to forward the additional packet flow to the second node, packets in said additional packet flow having a source address corresponding to the third node and a destination address corresponding to the second node, said step of generating an additional packet flow including at least one of a group of security steps which use the second shared secret, the group of security steps consisting of: encrypting a packet, adding an integrity check for the contents of the packet, and adding an authenticator check for the packet sender (column 7 lines 49 – 61 and column 8 lines 3 – 16).

Regarding claim 17, Srivastava discloses the method of claim 16, further comprising: operating the second node to communicate the first shared secret to the third node, the first shared secret being encrypted using the second shared secret (Figure 3 and column 11 lines 34 – 60).

Regarding claim 18, Srivastava discloses the method of claim 17, further comprising: mutually authenticating the second and third nodes prior to the second node transmitting the first shared secret to the third node (column 8 lines 17 – 34).

Regarding claim 22, Srivastava discloses a communications system for use with a second node, said communications system comprising: a first node including: memory means for storing a first secret, said first secret being shared between the first node and the second node to secure communications between said first and second nodes; and means for establishing a secure communications session with said second node using the first shared secret to secure the contents of packets communicated from the first node that are directed to the second node as part of a secure communications session; a third node, coupled to said first and second nodes, the third node including: memory means for storing a copy of said first shared secret; and means for receiving a secure flow of packets from the first node that are directed to said second node as part of the secure communications session (figure 1, column 2 lines 27 – 41 and column 9 lines 38 – 49).

Regarding claim 23, Srivastava discloses the communication system of claim 22, wherein said third node further includes: means for receiving from said second node the first shared secret; and means for storing the first shared secret in memory, said received first shared secret being encrypted using a second shared secret known to the second and third nodes (column 12 lines 24 – 55).

Regarding claim 25, 40, Srivastava discloses a method of operating a third node in a system comprising a first node, a second node and said third node, a first secret being shared between the first and second nodes to secure communications between said first and second nodes, the method comprising: receiving from said second node the first shared secret; storing said first shared secret in memory; and receiving a secure flow of packets from the first node that are re-directed away from said second node to said third node said redirected packets being packets which were originally directed to said second node as part of the secure communications session (figure 1, column 2 lines 27 – 41 and column 9 lines 38 – 49).

Regarding claim 42, 44 and 48, Srivastava discloses the method of claim 1, wherein the second node destination address is a Home Address of the second node (column 2 lines 27 – 4).

Regarding claim 49, Srivastava discloses the method of claim 47, further comprising: operating the third node to transmit another packet flow, said another packet flow including as a source address an address corresponding to the second node and including packets generated from said intercepted packets (column 7 lines 49 – 61 and column 8 lines 3 – 16).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2136

May 12, 2008
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135